

Notice of Allowability	Application No.	Applicant(s)
	09/675,113	HALE ET AL.
	Examiner	Art Unit
	Ronald Baum	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. This communication is responsive to 9/7/04.
2. The allowed claim(s) is/are 5,7-10,12,13,17-20,23,26,28-30 and 33.
3. The drawings filed on _____ are accepted by the Examiner.
4. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All
 - b) Some* c) None of the:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) including changes required by the Notice of Draftsperson's Patent Drawing-Review (PTO-948) attached
 - 1) hereto or 2) to Paper No./Mail Date _____.
 - (b) including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. Notice of References Cited (PTO-892)
2. Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____
4. Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. Notice of Informal Patent Application (PTO-152)
6. Interview Summary (PTO-413),
Paper No./Mail Date 09232004
7. Examiner's Amendment/Comment
8. Examiner's Statement of Reasons for Allowance
9. Other _____.



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with William W. Schaal, Reg. No. 39,018 on 9/07/2004.

1. Replace claims 5,7,12,13,23,26,28,30,33 with:

5. Embodied in a memory component, a digitally signed image comprising:
a post-relocation image being a result formed by alteration of a pre-relocation image of a software module upon loading of the image into the memory component;
information to convert the pre-relocation image to the post-relocation image, the information includes offsets for addressing routines within the software module and the offsets are generated after the software module is compiled and placed into an executable format; and
a digital signature based on the pre-relocation image, the digital signature is a hash value of the pre-relocation image digitally signed by a private key of a selected signatory.

7. The digitally signed image of claim 12, wherein the import table comprises a plurality of entries, each entry includes an identifier that indicates what segment of information contained in another digitally signed image is required by the image.

12. Embodied in a memory component, a digitally signed image comprising:
 - a Bound & Relocated Import Table (BRIT);
 - an import table;
 - an export table including a plurality of entries forming a listing of segments of information contained in the image, a selected entry of the plurality of entries includes an identifier of a segment of information associated with the segments of information, the selected entry further includes a second offset being an offset from a starting address of the digitally signed image to an address location of the segment of information;
 - an image of a software module; and
 - a digital signature based on the import table, the export table and the image.
13. A method comprising:
 - reconverting a post-relocation image of a digitally signed image back to a pre-relocation image, the pre-relocation image being an image of a software module prior to relocation where an address with the digitally signed image is changed;
 - conducting a one-way hash operation on the reconverted, pre-relocation image to produce a reconverted hash value;
 - recovering a hash value from a digital signature contained in the digitally signed image, the hash value is based on the pre-relocation image of the software module;
 - comparing the hash value to the reconverted hash value;
 - determining that an integrity of the post-relocation image remains intact if the hash value matches the reconverted hash value; and

determining that the post-relocation image has been modified beyond any modification caused by relocation when the hash value fails to match the reconverted hash value.

23. A method comprising:

verifying an integrity of a plurality of digitally signed images loaded in an electronic device, the plurality of digitally signed images includes a first digitally signed image and a second digitally signed image by

performing a hash operation on an import table, an export table and an image of the first digitally signed image to produce a first resultant hash value;

recovering a first hash value from a digital signature contained in the first digitally signed image,

comparing the first hash value with the first resultant hash value,

performing a hash operation on the import table, the export table and an image of the second digitally signed image to produce a second resultant hash value;

recovering a second hash value from a digital signature contained in the second digitally signed image, and

comparing the second hash value with the second resultant hash value;

determining whether an identifier in an import table of the first digitally signed image matches an identifier in the export table of the second digitally signed image; and

determining whether an entry of a Bound & Relocated Import Table (BRIT) corresponding to the identifier in the import table points to an address defined by the identifier in the export table.

26. An electronic device comprising:

a processor; and

a non-volatile memory component in communication with the processor, the non-volatile memory component includes including

a post-relocation image being an image of a software module altered during relocation in which an address associated with the image is adjusted before loading the post-relocation image into the memory component,

information to convert the image into the post-relocation image, the information placed within the non-volatile memory component includes an offset from a starting address of the image of the software module, and

a digital signature based on the image of the software module.

28. The electronic device of claim 30, wherein the import table loaded within the memory comprises a plurality of entries, each entry includes an identifier that indicates what segment of information contained in another digitally signed image is required by the image.

30. An electronic device comprising:

a processor; and

a memory in communication with the processor, the memory being loaded with a Bound & Relocated Import Table (BRIT), an import table, an export table, an image of a software module, and a digital signature based on the import table, the export table and the image, the

export table includes a plurality of entries forming a listing of segments of information contained in the image, a selected entry of the plurality of entries includes an identifier of a segment of information associated with the segments of information, the selected entry further includes a second offset being an offset from a starting address of the digitally signed image to an address location of the segment of information.

33. Embodied in a processor readable medium for execution by a processor, a software program comprising

a first software module to reconvert a post-relocation image of a digitally signed image back to a pre-relocation image, the pre-relocation image being an image of a software module prior to adjustment of an address corresponding to an address location allotted for the post-relocation image;

a second software module to conduct a hash operation on the reconverted, pre-relocation image to produce a reconverted hash value;

a third software module to recover a hash value from a digital signature contained in the digitally signed image, the hash value is based on the image of the software module;

a fourth software module to compare the hash value to the reconverted hash value;

a fifth software module to determine that an integrity of the post-relocation image remains intact if the hash value matches the reconverted hash value; and

a sixth software module to determine that the post-relocation image has been modified beyond any modifications caused by relocation when the hash value fails to match the reconverted hash value.

2. Cancel claims 1-4,6,11,14-16,21-22,24-25,27,31-32.

Examiner's Statement of Reasons for Allowance

3. Claims 5,7-10,12,13,17-20,23,26,28-30,33 are allowed over prior art.
4. This action is in reply to applicant's correspondence of 07 September 2004.
5. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.
6. As per claims 5,12,13,17,23,26,30,33, prior art of record, Wiedemer, U.S. Patent 4,796,181 fails to teach, alone, or in combination, of,

(claim 5) "Embodied in a memory component, a digitally signed image comprising:
a post-relocation image being a result formed by *alteration of a pre-relocation image of a software module* upon loading of the image into the memory component;
information to convert the pre-relocation image to the post-relocation image, the information includes *offsets for addressing routines within the software module* and the *offsets are generated after the software module is compiled and placed into an executable format*; and
a digital signature based on the pre-relocation image, the digital signature is a hash value of the pre-relocation image digitally signed by a private key of a selected signatory."

(claim 26) This is the system claim of claim 5 and appropriate analogous teachings apply.

(claim 12) "Embodied in a memory component, a digitally signed image comprising:

a Bound & Relocated Import Table (BRIT);

an import table;

an export table including a plurality of entries forming a listing of segments of information contained in the image, a selected entry of the plurality of entries includes an identifier of a segment of information associated with the segments of information, the selected entry further includes a second offset being an offset from a starting address of the digitally signed image to an address location of the segment of information;

an image of a software module; and

a digital signature based on the import table, the export table and the image."

(claim 30) This is the system claim of claim 12 and appropriate analogous teachings apply.

(claim 13) "A method comprising:

reconverting a post-relocation image of a digitally signed image back to a *pre-relocation image*, the pre-relocation image being an image of a *software module prior to relocation where an address with the digitally signed image is changed*;

conducting a one-way hash operation on the reconverted, pre-relocation image to produce a reconverted hash value;

recovering a hash value from a digital signature contained in the digitally signed image, the hash value is based on the pre-relocation image of the software module;

comparing the hash value to the reconverted hash value;
determining that an integrity of the post-relocation image remains intact if the hash value
matches the reconverted hash value; and
determining that the post-relocation image has been modified beyond any modification
caused by relocation when the hash value fails to match the reconverted hash value.”

(claim 33) This is the system claim of claim 13 and appropriate analogous teachings apply.

(claim 23) “A method comprising:
verifying an integrity of a plurality of digitally signed images loaded in an electronic device, the plurality of digitally signed images includes a first digitally signed image and a second digitally signed image by
performing a hash operation on an import table, an export table and an image of
the first digitally signed image to produce a first resultant hash value;
recovering a first hash value from a digital signature contained in the first digitally signed image,
comparing the first hash value with the first resultant hash value,
performing a hash operation on the import table, the export table and an image of
the second digitally signed image to produce a second resultant hash value;
recovering a second hash value from a digital signature contained in the second digitally signed image, and

comparing the second hash value with the second resultant hash value;
determining whether an identifier in an import table of the first digitally signed image
matches an identifier in the export table of the second digitally signed image; and
determining whether an entry of a Bound & Relocated Import Table (BRIT)
corresponding to the identifier in the import table points to an address defined by the identifier
in the export table.”

The *italicized* above claim elements dealing with (for example; claim 5) “*... a post-relocation image ... alteration of a pre-relocation image of a software module ... information to convert the pre-relocation image to the post-relocation image, ... offsets for addressing routines within the software module and the offsets are generated after the software module is compiled and placed into an executable format; ... a digital signature based on the pre-relocation image*” serving to patently distinguish the invention from prior art. Specifically, the use of post-altered compiled/executable software image data (i.e., via encoding, encryption, etc.) is taught in the prior art. However, as per the applicants arguments in the previous remarks in the Amendment (July 2, 2004), the examiner finds the applicant’s arguments to be persuasive in that the use of signing the image (pre-relocation) and relocation information so that the signature of the image can accommodate signature verification post relocation, (i.e., more specifically post compilation and post linking), patently distinguishes the invention from prior art. Claim 12 deals with multiple image referencing specifics via relocation information table entry aspects of the elements of claim 5 (and claim 13). Claim 13 deals with the reverse procedure (recovery) of claim 5, comprising the appropriate analogous elements. Claim 17 deals with the method of

building the table information of claim 12 elements, comprising the appropriate analogous elements. Claim 23 deals with the reverse procedure (recovery) of claim 17 table relocation information, comprising the appropriate analogous elements.

Dependent claims 7-10,18-20, 28-29 are allowable by virtue of their dependencies.

Conclusion

7. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100